Flow Based Intrusion Detection System Using Multistage Neural Network

Yousef Abuadlla, University of Al Jafara, Faculty of Electrical Engineering, abouadlla@gmail.com
Omran Ben Taher, Higher Institute of Technology and Science, Zliten, omalbeta@yahoo.com
Hesham Elzentani, Industrialization Center, Tripoli, Hesham342002@gmail.com

Abstract: *With the rapid expansion of computer networks during the past decade, security has become a crucial issue for computer systems. And to keep security at highest level, there is an increasing need for effective security monitors such as Network Intrusion Detection System to prevent such illicit. In the recent years many researchers focus their hard work on this field using different approaches to build dependable intrusion detection systems. One of these approaches is Flow-based intrusion detection systems that rely on aggregated network traffic flows. In this paper, Multistage Neural Network intrusion detection system based on aggregated flow data is proposed for detecting and classifying attacks in network traffic. The proposed system detects significant changes in the traffic that could be a possible attack in the first stage of neural network, while the second stage has the ability to recognize an attack, to differentiate one attack from another i.e. classifying attack, and the most important, to detect new attacks with high detection rate and low false negative. Two different neural network structures with the use of different training algorithms have been used in our proposed Intrusion Detection System. The experimental results show that the designed system is promising in terms of accuracy and low probability of false alarms, where the overall accuracy classification rate average is equal to 99.25%.*

Keywords: Artificial neural network, Intrusion Detection, Netflow, Anomaly detection.

1. Introduction

With the enormous growth of network-based computer services and the huge increase in the number of applications running on networked systems. Moreover the use of computers in the home and in business was increased considerably. As a result, security becomes a big and increasingly-important issue for all networks and computer in today's enterprise environment. Internet (as many other things) is double-edged. It is the entrance to many beneficial things. Unfortunately, it also opens the way for a lot of harmful things to login into your device. Hackers and intruders have made many successful attempts to bring down high-profile companies networks and systems. Many methods have been developed to secure the system infrastructure and communication over the internet such as the use of firewalls, intrusion detection, and encryption [8], [36].

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusion. It aims to protect the confidentiality, integrity, and availability of critical networked information systems [37], [39]. Intrusion detection system (IDS) is a system that gathers and analyzes information from various areas within a computer or a network to identify attacks made against these components. IDS is an important component for security system. It complements security of other technologies through the provision of information for management. It does not only detect attacks that are discovered by other security elements, but also attempts to provide notification of new attacks that cannot be expected by the other ingredients. This is done by continuously monitoring and analyzing the events that occur in the computer system or network from inside or outside.

In general, IDS uses a number of generic methods for monitoring the exploitations of vulnerabilities. IDSs can be characterized by depending on three main aspects [16], [33]:

- The data source: In this case, we have host-based, network-based, or hybrid IDSs. Host based IDS monitors' computer components (such as operating system, packet, system log, etc.). Network based IDS monitors the network (such as traffic). Hybrid IDS combines host with network for monitoring computer and network together.
- The model of intrusion detection: Here we have anomaly detection, misuse detection, or hybrid detection. Anomaly based IDS monitoring depends on the behaviour of system. Misuse based IDS monitoring depends on signature to data. Hybrid techniques combine anomaly with misuse.

- The audit collection and analysis: Here IDSs are divided into either centralized or decentralized (distributed) IDSs. In centralized IDSs, monitoring, detection, and reporting are controlled directly from a central location. In decentralized IDSs, monitoring and detection are controlled from a local control node with hierarchical reporting to one or more central location(s).

IDS has become increasingly important in recent years to handle the growing number of attacks, the rise in the amount of traffic as well as the increase in line speed [35]. Well-known systems like Snort [30] and Bro [31] exhibit high resource consumption when confronted with the overwhelming amount of data found in high-speed of today networks [32]. The constant increase in network traffic and the fast introduction of high speed network equipment [14] make it hard to maintain traditional packet based intrusion detection systems. Given these problems, flow-based approaches seem to be promising candidates for intrusion detection research. Flows are monitored by specialized accounting modules usually placed in network routers. These modules are responsible for exporting reports on flow activity to external collectors. Flow-based IDSs will analyze these flows to detect attacks. Compared to traditional IDSs, flow-based IDSs have to handle a considerably lower amount of data. And according to previous researches, approaches that rely on aggregated traffic metrics, such as flow-based approaches, show improved scalability and therefore seems more likely. The benefit of flow-based approaches is that only a fraction of the total amount of data needs to be analyzed. It provides an aggregated view of the data transferred over the network and between hosts, in terms of number of packets, bytes and measured flows themselves.

A flow is defined as a unidirectional stream of packets that share common characteristics, such as source and destination addresses, ports and protocol type. Additionally a flow includes aggregated information about the number of packets and bytes belonging to the stream, as well as its duration. Flows are often used for network monitoring, allowing us to obtain a real time overview of the network status; common tools for this purpose are Nfsen [27] and Flowscan [28], while the *de facto* standard technology in this field is Cisco Netflow, particularly its versions 5 and 9 [5].

The computational changes in the last several decades have brought growth to new technologies. One of these technologies is artificial neural networks (ANNs). Over the years, ANNs have given various solutions to the industry. Designing and implementing intelligent systems have become an important activity for the innovation and development of better products for human life. Examples might include the case of the implementation of artificial life and giving solution to interrogatives that linear systems are not able to resolve [34]. Neural Networks have strong discrimination and generalization abilities, when utilized for classification purposes [2]. An increasing amount of research in the last few years has investigated the application of Neural Networks to intrusion detection. If properly designed and implemented, Neural Networks have the potential to address many of the problems encountered by rule-based approaches. Neural Networks were specifically proposed to learn the typical characteristics of system's users and identify statistically significant variations from their established behavior. In order to apply this approach to Intrusion Detection, we would have to introduce data representing attacks and normal network flow to the Neural Networks to adjust the coefficients of these Networks automatically during the training phase. In other words, it will be necessary to collect data representing normal and abnormal behavior to train the Neural Networks. After training has been accomplished, a certain number of performance tests with real network traffic and attacks have been conducted [26]. In our study two different neural network methods have been used for our intrusion detection system: Multi Layer Perceptron (MLP) neural network, and Radial Basis Function Network (RBFN).

The ANN needs to be trained (or learned) in order to reach the best output. Basically, learning is a process by which the free parameters (i.e., synaptic weights and bias levels) of the ANN are adapted through a continuing process of stimulation by the environment in which the network is embedded. The type of learning is determined by the manner in which the parameter changes take place. In a general, the learning process may be classified as supervised or unsupervised. The most used training algorithm is back propagation algorithm gradient descent (GDA) with the disadvantage of slow training while Levenberg-Marquardt [11], [12] is one of the accurate algorithms and faster than GDA, but consumes more memory space. In the other hand The RBFN offers a viable alternative to the two-layer neural network in many applications of signal processing, decision making algorithms, pattern recognition, control, and function approximation. It has been shown that the RBFN can fit an arbitrary function with just one hidden layer [13], but they cannot quite achieve the accuracy of the back-propagation

network. Although, RBFN can be trained several orders of magnitude faster than the back-propagation network, and this is a very important advantage in real or semi real time applications.
In our study, flow-based intrusion detection and classification system is implemented using multistage neural network. While in many previous studies [6], [32], [22] the implemented system is a neural network based on DARPA [7] or KDD'99 [18] dataset with the capability of detecting normal or abnormal connections, in our study a more general problem is considered in which the attack type is also classified and the training dataset is based on flow dataset instead of DARPA dataset.

This paper is organized as follows, section 2 present an overview of a number of related works, section 3 explains the proposed system , section 4 evaluate the proposed system, and section 5 discusses the experiments results followed by conclusions and future work.

2. Related Work

With the speedy rising of network speed, flow-based techniques attracted the concern interest of researchers, especially in analysis of high-speed networks. And day to day increase in network usage and load, have clearly pointed out that scalability is a growing problem. In this situation, flow based solutions to monitor and, moreover, to detect intrusions help to solve the problem. They achieve, indeed, data and processing time reduction, opening the way to high-speed detection on large infrastructures. Sperotto et al. [35] provided a comprehensive survey on current research in the domain of flow-based network intrusion detection. Gao and Chen [10] designed and developed a flow-based intrusion detection system. Karasaridis et al. [17], Shahrestani et al.[38]. A sound evaluation of a neural network based IDS requires high-quality training and testing datasets. Unfortunately, the de facto standard is still the DARPA data set created by Lippmann et al. [19]. Despite its severe weaknesses and the critique published by McHugh [20], it is still used. The KDD'99[18] data set can be regarded as another popular data set. Sperotto et al. [40] contributed the first labelled flow-based dataset intended for evaluating and training network intrusion detection systems.

Several Neural Network approaches were employed for Intrusion Detection systems based on netflow and DARPA [7] dataset. Muna Mhammad T. Jawhar [21] used Neural Network and Fuzzy C-Mean (FCM) clustering algorithms. Rodrigo Braga [4] used OpenFlow and the SOM unsupervised neural network. Vallipuram and Robert [42] used back-propagation Neural Network having all features of KDD (Knowledge Discovery in Databases) data [18]. Tie and Li [45] used the back propagation (BP) network with Genetic Algorithms (GAs) to enhance BP, for selected attacks and some features of the KDD dataset as input. Mukkamala, Andrew, and Ajith [23] used Back Propagation Neural Network with many types of learning algorithm. Jimmy and Heidar [15] used Neural Network for classification of unknown attacks. Novikov, Roman, and Reznik [25] used MLP and Radial Based Function (RBF) Neural Network for classification of five types of attacks. Ahmed, Ullah and Mohsin [1] used Resilient Back propagation algorithm for detecting network intrusion attacks in a precise way by using the power of RPROP ((Resilient Back propagation) learning algorithm. B. Subba, S. Biswas and S. Karmakar [46] used Neural Networks for attack classification. D, Vrushali & Pawar [47] developed Anomaly Detection System based on back propagation Neural Networks.

3. Proposed Approach

The proposed system for flow-based intrusion detection is composed of four main stages, as depicted in Figure 1. These stages are Feature extraction stage, Detection stage, Classification stage, and Alert stage. More details of these stages are presented in the following subsections.

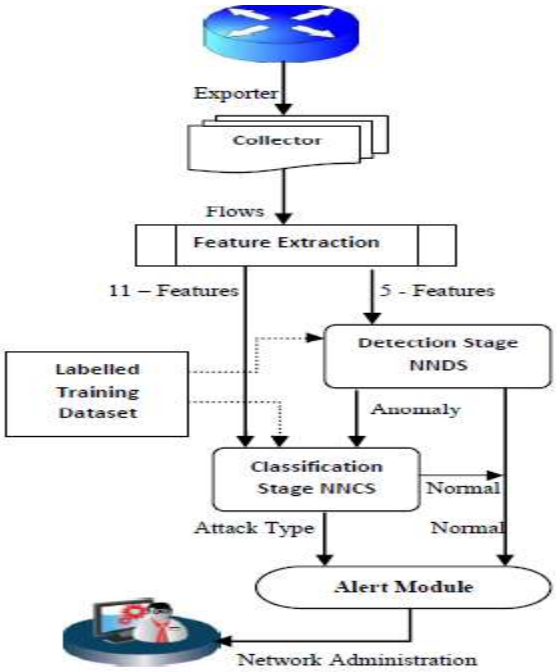

Figure 1: Proposed Multistage NN Based System.

3.1. Feature Extraction Stage

The Feature Extraction stage starts after the monitor completes capturing the packets that passed through the network. The packets can be captured at the network layer (IP) and/or the transport layer (TCP, UDP, ICMP). All unidirectional streams of packets that share common characteristics, such as source and destination addresses, ports and protocol type are collected and extracted as flows according to the Cisco protocol [5]. The feature extraction module and after receiving collected and extracted flows start applying predefined processes to extract most features that are important for anomaly intrusion detection, and classification stage, and gathers them in 5-*tuples and 11-tuples* that are passed to the detection and classification stages respectively. Table 1 gives a more detailed explanation for all features of both stages. Pre-processing must be done on all selected features before passing them to the both stages; this phase involves normalizing all features by mapping all the different values for each feature to [0, 1] range.

Table 1: Proposed system feature description.

No	Feature	Neural Network Stage	Description
1	AFS	NNCS	Average Flow Size, it's often very small in order to increase the efficiency of attacks
2	APS	NNDS,NNCS	Average Packet Size, low average size is a sign for anomaly, for ex. In TCP flood attack packet of size 120 byte is typically sent
3	APN	NNDS,NNCS	Average Packet Number, a small packet number is a feature of IP spoofing in Dos attack(ex. 3 packets)
4	FSDIP	NNDS,NNCS	Number of Flows to the Same Destination IP, a high number of flows could mean a flood or port scan attack
5	FDDP	NNCS	Number of Flows to Different Destination port, high number could be a port scan attack
6	LAND	NNDS,NNCS	Land attack (SrcIP=DstIP, SrcPort=DstPort)
7	SYS – SYS/ACK	NNDS,NNCS	By comparing number of SYN and SYN/ACK packets that a host received and returned respectively, this feature was used by many researchers [44] to detect Dos attack
8	FSSIP	NNCS	Number of Flows from the Same Source IP, attacker can send for example ICMP ping packet to every possible address within a subnet
9	FDSIP	NNCS	Number of Flows from Different Source IP, IP spoofing is wildly used by attackers, high number of different ip addresses within a short period of time could be a strong sign for attack(Dos)
10	FSDP	NNCS	Number of Flows to the Same Destination Port, in some cases the attacker sends GET request to some ports only (ex. Port 80) to crash the server.
11	PT	NNCS	Protocol Type (TCP, UDP, and ICMP), with the combination to the all previous features can help to determine the type of attack.

3.2. Neural Network Based Detection stage

Anomalies in our system are defined as unusual activities in the network. The purpose of Neural Network Detection stage one (NNDS) is to find out such activities using a small number of features extracted from collected flow raw data. The number of input nodes of the NNDS corresponds to the number of the selected features (5 Features). The implemented NNDS includes one input layer, one hidden layer and an output layer of 2 nodes as shown in figure 2 (01 as normal traffic, and 10 as anomaly traffic)). The numbers of hidden layers and nodes in them have been determined based on the back propagation (BP) computation process and the process of trial and error which took stretched time. Algorithm 1 below is a simplified general description of the detection process.

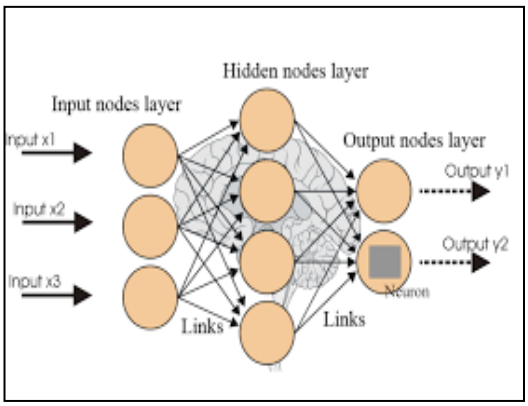

Figure 2: Multi layer Feedforword Neural network architecture

Algorithm 1: Detection Module

While (new data available) do

- *Read 5-tuple inputs for NNDS*
- *Feed parameters to the NNDS*
- *NNDS creates the following results:*

  If the data is "normal", then
- *Assign 01 to the output of NNDS*

  Else
- *Assign 10 to the output of NNDS as anomaly traffic*
- *Call neural network classification (NNCS)*

End while

3.3. Neural Network Based Classification Stage

There are several classification techniques that can be used for classifying attacks based on flow data such as Neural Networks, statistical methods, genetic algorithms, and others. In our system, neural network have been used in classification of data. The results can only be obtained after completing both of training and testing phases. The result from the neural network classification stage is classified into five possible categories. Table 2 maps these categories to the actual outputs from Neural Network Classification Stage (NNCS).

Table 2: Neural network classified categories.

No	Category	NN2 Outputs
1	Dos/DDos Attack	10000
2	Port Scan Attack	01000
3	Land Attack	00100
4	Other/unknown Attack	00010
5	Normal	00001

The number of input nodes to the NNCS corresponds to the number of the selected features (11 Features). The implemented neural network includes one input layer, one hidden layer and an output layer of 5 nodes as shown in figure 3 (table 2 contains the descriptions of the outputs). The numbers of nodes in the hidden layers has been determined based on the back propagation (BP) computation process and the process of trial and error. Algorithm 2 describes the Classification procedure.

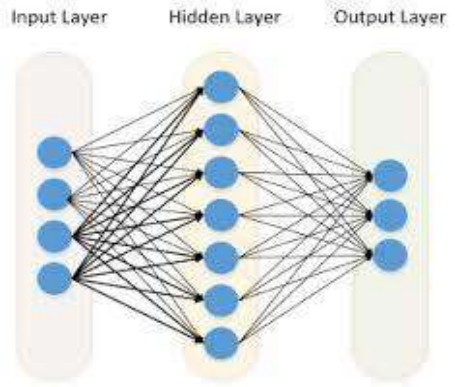

Figure 3: one input layer, one hidden layer, and an output layer neural network.

Algorithm 2: Classification Procedure

While (activated from NNDS) do

Begin

- *Read 11-tuple inputs for NNCS*
- *Feed parameters to the NNCS*
- *NNCS creates the following results:*

  If data is "normal", then

- *Assign 00001 to the output of NNCS*

  Else

- *Assign appropriate attack type to the output of NNCS according to the table 2*
- *Enable Alert Module*

End

3.4. Alert Stage

This is the final stage of the proposed system. This stage involves identifying the events that occurred whether abnormal or not, then sending the required signals according to the output from NNCS to alert administrator and creates alarms when appropriate.

4. Experimental Results

The proposed system has been implemented and experimentally evaluated using MATLAB (R2011b) neural network Toolbox. Figure 4 represents the block diagram of the implemented system. The considered scenarios in our experiments are as follows:

A. Packet capturing process: it is the first step in the system operation, enables to capture the incoming and outgoing packets in the network.

B. Collecting and exporting flows: in this phase all unidirectional streams of packets that share common characteristics, such as source and destination addresses, ports and protocol type are collected and extracted as flows according to the Cisco protocol [5].

C. Feature extraction process: Pre-processing must be done on all selected features before passing them to the both stages, such as mapping and normalization.

D. Machine training: The ANN was trained by pre-processed NetFlow dataset, different number of iterations and hidden units to determine the level of training. And to find out when the neural network was trained properly to detect attacks. Also number of algorithms has been used for training and testing neural networks to detect and classify various actions. After the training of the ANN and finding the best detection rate, the best weights have been saved in a file to be used during the testing phase. The Detection Rate

(DR) and False Positive rate (FP) have been calculated for different scenarios according to the following formulas:

DR = NA / TA * 100[%]

FP = CA / NT * 100[%]

Where:

DR: Detection Rate

NA: Number of detected Attacks.

TA: Total number of Attacks.

FP: False Positive.

CA: number of normal Classified as Attack.

NT: total Number of normal Traffic

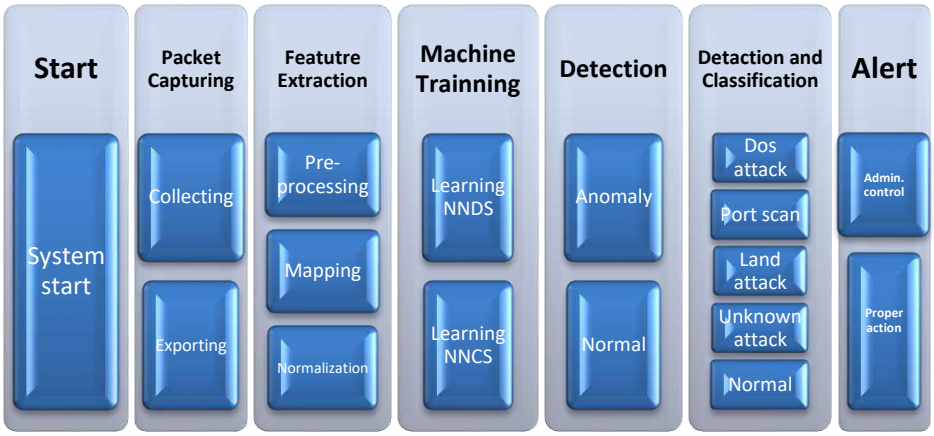

Figure 4. Block diagram of the implemented system.

E. Detection phase: This stage includes detection of attacks by deciding whether flows are normal or abnormal. The training and testing have been performed with five selected features. One input layer, one hidden layer, and one output layer has been used in NNDS.

The experiments have three phases namely: a training phase, a validation phase and a testing phase. All experiments in this stage were done with 101806 records of attack traffic, and 48556 of normal traffic. 29088 records were used for testing the neural network and it contains 18635 records of attack traffic, and 10453 records of normal traffic. Detection Rate and False positive Rate are shown in Table 3. Figure 5 shows the performance of detection module.

Table 3: Results of Detection Module (NNDS).

Parameters	Test 1	Test 2	Test 3
Hidden Layer	50	50	20
Training function	Resilient Back propagation	Levenberg-Marquardt	Radial Basis Function Net.
Number of detected attacks	17276	17553	16976
Number of detected traffic as normal	9691	9836	9552
Detection Rate	92.712%	94.1%	91.1%
False positive Rate	7.3%	5.9%	8.9%

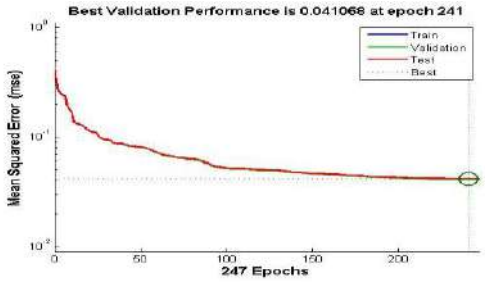

Figure 5: Performance of the detection module

F. Classification Phase: This scenario includes detection of packets, and classifies them as a normal traffic, or one of the four main attack types (DOS/DDOS, Port Scan, Land attack, or other/unknown attack). 11 selected features were used for training and testing the neural network. All experiments in this stage have been done with 101806 records of attack traffic, and 48556 of normal traffic. 21816 records were used for testing the neural network and it contains 14527 records of attack traffic, and 7289 records of normal traffic. Detection Rate and False positive Rate are shown in Table 4. Figure 6 shows the performance of the classification module. During the testing phase, the classification rate (CR) of each attack types was calculated as shown in table 5 according to the following formula:

CR = NC / AT * 100[%]

Where:

CR: Classification Rate.

NC: Number of Classified attack.

AT: total number of Attack Type

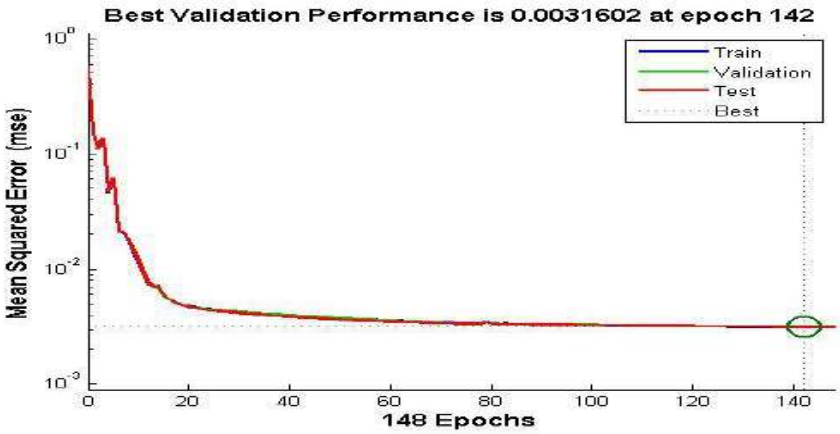

Figure 6: Performance of the classification module

Table 4: Results of Classification Stage (NNCS)

Parameters	Test 1	Test 2	Test 3
Hidden Layer	80	80	40
Training Function	Resilient Back propagation	Levenberg-Marquardt	Radial Basis Function Net.
Number of detected attacks	14294	14443	13858
Number of detected traffic as normal	7172	7235	6953
Detection Rate	98.4%	99.25%	95.3%
False positive Rate	1.6%	0.75%	4.6%

Table 5. Classification Rate (NNCS)

Attack Name	Number of attacks	Classified attacks	Classification rate
Dos/DDos	4490	4490	100%
Port Scan	9929	9919	99.9%
Land	85	85	100%
Unknown	23	18	78%
Normal	7289	7246	99.4%

5. Discussion and Comparison of Results

Intrusion detection system using multistage neural network and based on flow dataset have been proposed and tested. Three different training algorithms (Levenberg-Marquardt, Radial Basis Function net, and Resilient Back propagation) were used for training both neural networks. Detection Stage (NNDS) was trained until the best validation performance 0.0410 was met at epoch 247 as shown in figure 5. The results in Table 3 show that the detection rate is 94.1% with false positive of 5.9%. On the other hand results from classification stage (NNCS), show significantly larger improvement of prediction accuracy than the detection stage. Figure 6 shows that, the best validation performance 0.0031 was met at epoch 148.Table 4 shows that, the detection rate relatively high at 99.25% for MLP, and 95.3% for RBF detection algorithm. The false alarms were as low as 0.588% in MLP neural network and 4.6% in RBF neural network. Table 5 shows that, the classification rate comparatively high of Dos attack, port scan attack, land attack, and unknown attack were detected and classified correctly by using Multistage neural networks. The analysis of both layer results show that MLP with Levenberg-Marquardt is found to be fast compared to Resilient Back propagation, low memory consumption compared to Radial Basis Function, and low in false alarms.

According to the recently published results [42], [23], [25], [41], [21], [4], [9], [29], [3] and our result based on neural networks, found that our proposed IDSs are greatly competitive with others and Figure 7 indicates that our system has possibilities for detection and classification of computer attacks with the minimum number of extracted features from flow dataset.

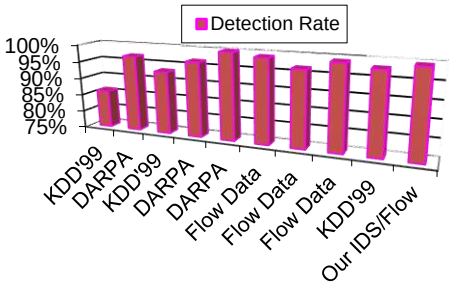

Figure 7: Detection Rate [%]

6. Conclusion and Future Work

A flow based intrusion detection and classification system using multistage neural networks was proposed. One neural network detects traffic anomalies and the other one classifies the type of attack. This system can easily be extended, configured, and modified by replacing some features or adding new features for new types of attacks.
The experimental results with our proposed IDS showed that the use of Flow dataset and extracting only features that significantly contribute to intrusion detection gives promising results. The obtained detection rate (94.1% for anomaly detection at stage one, and 99.25% for classification at stage two) is remarkably good compared to other approaches that are based on a similar approach using the same type of training dataset.
The MLP network has a better classification ability compared to RBFN, but memory and time consumption is 3-5 times greater. Otherwise, RBFN has a simple architecture and hybrid learning algorithm which leads to less time/memory consumption and it is better for working in real-time and for retraining with new data.
Our future research will be directed towards developing a more accurate model that can be used in real-time for detecting and classifying anomaly with minimum features and less training time.

References

[1] Ahmad I., Ullah S., Swati, and Mohsin S., "Intrusions Detection Mechanism by Resilient Back Propagation (RPROP)", *European Journal of Scientific Research*, vol. 17, No.4, pp. 523-531, 2007.
[2] Al-Subaie M., "The power of sequential learning in anomaly intrusion detection", *degree master thesis*, Queen University, Canada.2006.
[3] Alsharafat W., "Applying Artificial Neural Network and eXtended Classifier System for Network Intrusion Detection", *The International Arab Journal of Information Technology*, vol. 10, No. 3, pp. 230-238, 2013.

[4] Braga R., Mota E., and Passito A.," Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow", *35th Annual IEEE Conference on Local Computer Networks*, LCN 2010, Denver, Colorado 6, 2010.
[5] Cisco, "IOS NetFlow Configuration Guide", Available at: www.cisco.com, April 2008.
[6] Cannady J., "Artificial neural networks for misuse detection," *Proceedings of the 1998 National Information Systems Security Conference*, Arlington, VA, 1998.
[7] DARPA1998, Available at: http://www.ll.mit.edu/IST/ideval/docs/1998.
[8] D. Herrmann, "A practical guide to security engineering and information assurance", 2002, www.auerbach-publications.com.
[9] Govindarajan M., and Chandrasekaran R., "Intrusion detection using neural based hybrid classification methods", *Computer Networks Journal*. Vol. 55, No. 8, pp. 1662-1671, 2011.
[10] Gao Y, Li Z., and Chen Y., "A DoS Resilient Flow-level Intrusion Detection Approach for High-speed Networks", *in Proc. of the 26th IEEE International Conference on Distributed Computing Systems*, Washington, USA, pp.39, 2006.
[11] Hagan M, Demuth H., and Beale M., *Neural Network Design*, Boston, MA: PWS Publishing, 1996.
[12] Hagan M., and Menhaj M., "Training feed-forward networks with the Marquardt algorithm", *IEEE Transactions on Neural Networks*, Vol. 5, No. 6, pp. 989–993, 1994.
[13] Hartman E., Keeler J., and Kowalski J., "Layered neural networks with Gaussian hidden units as universal approximations*". Neural Computation Journal*, vol. 2, pp. 210–215, 1990.
[14] Internet2 NetFlow: Weekly Reports. netflow.internet2.edu/weekly, April 2008
[15] Jimmy S. and Heidar A., "Network Intrusion Detection System using Neural Networks*", IEEE computer society*, Vol. 05, pp. 242-246, 2008.
[16] J. Daejoon , H. Taeho, and H. Ingoo "The neural network models for IDS based on the asymmetric costs of false negative errors", Pergamon, Journal of Expert Systems with Applications, No. 25, pp. 69–75, 2003.
[17] Karasaridis A., Rexroad B., and Hoeflin D., "Wide-scale botnet detection and characterization", *in* Proc. *of the first conference on Hot Topics in Understanding Botnets (HotBots '07)*, Berkeley, CA, USA, p.7, 2007.
[18] KDDCup1999, Available at: http://kdd.ics.uci.edu/databases.
[19] Lippmann R. ., "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation," *in Proc. of the DARPA Information Survivability Conference and Exposition*, pp. 12-26, 2000.
[20] McHugh J., "Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory," *ACM Transactions on Information and System Security*, vol. 3, no. 4, pp. 262 – 294, 2000.
[21] Muna J., M. and Mehrotra M., "Design Network Intrusion Detection System using Fuzzy-Neural Network", *International Journal of Computer Science and Security*, vol. 4, no. 3, pp. 285-294, 2010.
[22] Mukkamala S., "Intrusion detection using neural networks and support vector machine", *Proceedings of the 2002 IEEE International*, Honolulu, HI, 2002.
[23] Mukkamala S., Sung A., and Abraham A., "Intrusion detection using an ensemble of intelligent paradigms", *Journal of Network and Computer Applications*, pp. 167–182, 2005.
[24] Muna J., M. and Mehrotra M., "Intrusion Detection System: A design perspective", *2nd International Conference on Data Management*, IMT Ghaziabad, India, 2009.
[25] Novikov D., Roman V., Yampolskiy, and Reznik L., "Anomaly Detection Based Intrusion Detection", *IEEE Third International Conference on Communication, Networking & Broadcasting*, ITNG, pp 420-425, 2006.
[26] Novikov D., Roman V., Yampolskiy, and Reznik L, "Artificial Intelligence Approaches for Intrusion Detection", *IEEE Long Island Systems Applications and Technology Conference*, pp. 1-8, 2006.
[27] Net flow sensor, Available at: www. nfsen.sourceforge.net.
[28] Plonka D., "Flowscan", Available at: www.caida.org/tools/utilities/flowscan, April 2008.
[29] Prasanta G., Bhattacharyya D., Borah B., and K. Kalita, "MLH-IDS: A Multi-Level Hybrid Intrusion Detection Method", *The Computer Journal Advance Access*, 2013.
[30] Paxson V., "Bro: a system for detecting network intruders in real-time", *in the Proceedings of the 7th USENIX Security Symposium*, San Antonio, Texas , pp. 2435–2463, 1998.
[31] Roesch M., "Snort & intrusion detection system", Available at: http://www.snort.org, 2010.
[32] Ryan J., Lin M., and Miikkulainen R., "Intrusion Detection with Neural Networks," *AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 AAAI Workshop*, Providence, RI, pp. 72-79, 1997

[33] R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems", 2002.
[34] R. Ghosh, "A novel hybrid learning algorithm for artificial neural networks", Ph.D. Thesis, School of Information Technology, Griffith University, 2002.
[35] Sperotto A., Schaffrath G., Sadre R., Morariu C., Pras A., and Stiller B.," An overview of ip flow-based intrusion detection". *IEEE Communications Surveys &Tutorials*, vol. 12, no 3 pp. 343–356, 2010.
[36] S. Kiran, "Exploring a novel approach for providing software security using soft computing systems", International Journal of Security and Its Applications, Vol. 2, No. 2, pp. 51- 58, 2008.
[37] S. Alexander, "An anomaly intrusion detection system based on intelligent user recognition", Ph.D. Thesis, Faculty of Information Technology, University of Jyväskylä, Finland, 2002.
[38] Shahrestani A., Feily M., Ahmad R., and Ramadass S., "Architecture for Applying Data Mining and Visualization on Network Flow for Botnet Traffic Detection," in *Proc. of the International Conference on Computer Technology and Development*, Washington, DC, USA, pp. 33-37, 2009.
[39] S. Mansour and A. Sha'bani, "Fast neural intrusion detection System Based on Hidden Weight Optimization Algorithm and Feature Selection", World Applied Sciences Journal, No. 7 (Special Issue of Computer & IT), pp. 45-53, 2009.
[40] Sperotto A., Sadre R., Vliet F., and Pras A, "A Labeled Data Set for Flow-Based Intrusion Detection," *in Proc. of the 9th IEEE International Workshop on IP Operations and Management*, Berlin, pp. 39 – 50, 2009.
[41] Sammany M., Sharawi M., El-Beltagy M., and Saroit I. "Artificial neural networks architecture for intrusion detection systems and classification of attacks". *Accepted for publication in the 5th international conference INFO2007*, Cairo University, 2007.
[42] Vallipuram M., and Robert B., "An Intelligent Intrusion Detection System based on Neural Network", *IADIS International Conference Applied Computing*, 2004.
[43] V. Konstantinos, "Machine learning approaches to medical decision making ", PhD Thesis, Department of Computer Science, University of Bristol. March 2001
[44] Wang H., Zhang D., and Shin K.,"SYN-dog: Sniffing SYN Flooding Sources", *In Proc. of 22nd International Conference on Distributed Computing Systems*, Vienna, Austria, 2002.
[45] Zhou T., and Yang L., "The Research of Intrusion Detection Based on Genetic Neural Network", *In Proceedings of the 2008 International Conference on Wavelet Analysis and Pattern Recognition*, Hong Kong, 2008.
[46] B. Subba, S. Biswas and S. Karmakar, "A Neural Network based system for Intrusion Detection and attack classification," *2016 Twenty Second National Conference on Communication (NCC)*, Guwahati, 2016, pp.1-6.doi: 10.1109/NCC.2016.
[47] D, Vrushali & Pawar, Anomaly based IDS using Backpropagation Neural Network. International Journal of Computer Applications.2016, 136. 29-34. 10.5120/ijca2016.